

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)	
)	
Anthony C. FASCENDA)	Group Art Unit: 2131
)	
Application No.: 10/679,371)	Confirmation No.: 4292
)	
Filed: October 7, 2003)	Examiner: Shin Hon CHEN
)	
For: LOCALIZED NETWORK)	
AUTHENTICATION AND)	
SECURITY USING TAMPER-)	
RESISTANT KEYS)	

APPEAL BRIEF

TABLE OF CONTENTS

	<u>Page</u>
I. REAL PARTY IN INTEREST	1
II. RELATED APPEALS AND INTERFERENCES.....	1
III. STATUS OF CLAIMS	1
IV. STATUS OF AMENDMENTS	2
V. SUMMARY OF CLAIMED SUBJECT MATTER	2
A. SUMMARY OF INDEPENDENT CLAIM 1	2
B. SUMMARY OF DEPENDENT CLAIM 2	3
C. SUMMARY OF INDEPENDENT CLAIM 13	3
D. SUMMARY OF INDEPENDENT CLAIM 19	4
E. SUMMARY OF DEPENDENT CLAIM 25	4
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	5
VII. ARGUMENTS.....	5
A. THE OFFICE ACTION APPEARS TO IMPERMISSIBLY COMBINE MULTIPLE EMBODIMENTS OF PITCHENIK	5
B. CLAIMS 1, 2, 19 AND 25 ARE PATENTABLE OVER PITCHENIK IN VIEW OF EBERHARD UNDER 35 U.S.C. § 103.....	7
1. Claim 1 Is Patentable Over Pitchenik In View Of Eberhard Under 35 U.S.C. § 103	7
i. Pitchenik Fails To Disclose The Protocol Steps Of Claim 1	8
ii. Eberhard Fails To Disclose Generating A Second Random Number Different From A First Random Number	10
iii. The Office’s Motivation To Combine Is Flawed.....	11
2. Claim 2 Is Patentable Over Pitchenik In View Of Eberhard Under 35 U.S.C. § 103	12
3. Claim 19 Is Patentable Over Pitchenik In View Of Eberhard Under 35 U.S.C. § 103	13

i.	Pitchenik Fails To Disclose The Protocol Steps Of Claim 19	14
ii.	Eberhard Fails To Disclose Generating A Second Random Number Different From A First Random Number	16
iii.	The Office’s Motivation To Combine Is Flawed.....	17
4.	Claim 25 Is Patentable Over Pitchenik In View Of Eberhard Under 35 U.S.C. § 103	18
C.	CLAIM 13 IS PATENTABLE OVER PITCHENIK IN VIEW OF EBERHARD AND FURTHER IN VIEW OF SHTEYN UNDER 35 U.S.C. § 103.....	18
1.	Pitchenik Fails To Disclose A Physical Token	19
2.	Pitchenik Fails To Disclose Tamper-Resistance	20
3.	Shteyn Fails To Disclose Tamper-Resistance.....	21
4.	Shteyn Fails To Disclose A Physical Token Comprising A Random Number Generator.....	22
5.	Eberhard Fails To Disclose Generating A Second Random Number Different From A First Random Number.....	22
6.	The Office’s Motivation To Combine Eberhard With Pitchenik Is Flawed	23
7.	The Office’s Motivation To Combine Shteyn With Pitchenik And Eberhard Is Flawed	24
VIII.	CONCLUSION.....	25

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)	
)	
Anthony C. FASCENDA)	Group Art Unit: 2131
)	
Application No.: 10/679,371)	Confirmation No.: 4292
)	
Filed: October 7, 2003)	Examiner: Shin Hon CHEN
)	
For: LOCALIZED NETWORK)	
AUTHENTICATION AND)	
SECURITY USING TAMPER-)	
RESISTANT KEYS)	

APPEAL BRIEF

In response to the Notice of Panel Decision from Pre-Appeal Brief Review mailed June 29, 2006, Appellant respectfully requests that the Board of Patent Appeals and Interferences ("Board") withdraw the rejections of record and allow the pending claims, which are attached hereto as an Appendix.

I. REAL PARTY IN INTEREST

The real party in interest is Koolspan, Inc., which is the current assignee of the above-referenced application.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1-11 and 13-28 are pending and stand rejected. Claim 12 has been cancelled. The rejections of claims 1-11 and 13-28 are appealed.

IV. STATUS OF AMENDMENTS

No amendments to the claims have been filed subsequent to the last Office Action (hereinafter, “Office Action”), which was mailed November 14, 2005. Appellant filed the Notice of Appeal on March 14, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention, as claimed, is directed to a cryptographic protocol. *See, e.g.*, Specification, ¶¶ 3, 13, and 14. Such protocols are useful for, *e.g.*, authenticating computing devices present on a publicly-accessible network. *See, e.g.*, Specification, ¶¶ 17 and 18. Such authentication typically ensures that a communicating device is authentic. *Id.* That is, the claimed cryptographic protocols may be used to ensure that a device on the other end of a communication channel is the actual device with which a user intends to communicate. *Id.*

In general, cryptographic protocols are delicate creatures. Each is designed to carefully avoid multiple “attacks” at each stage. Such attacks may be directed to determining a cryptographic key, determining a plaintext message, or impersonating a user or device. At each stage in a protocol, the communicated parameters are carefully selected in order to thwart such attacks. Importantly, it will typically void the security of a protocol to add, remove, or swap out parameters willy-nilly.

A. SUMMARY OF INDEPENDENT CLAIM 1

The present invention as recited in claim 1 provides a cryptographic protocol for authentication. For support, *see* Fig. 10, ¶¶ 56-59 and 61. The protocol comprises an exchange of carefully-selected parameters by two communicating parties. Specifically, claim 1 recites a “method of authenticating computing devices on a communications network.” *See, e.g.*, Specification, ¶¶ 17

and 18. The party wishing to authenticate the computing device receives a first challenge from the computing device, where the first challenge includes an encrypted first random number and a unique identifier associated with the computing device. *See, e.g.*, Specification, Figs. 9A, 9B, 10, and ¶ 59. A first secret cryptographic key associated with the unique identifier is obtained. *Id.* A second random number is generated, where the second random number is different from the first random number. *See, e.g.*, Specification, Figs. 9A, 9B, 10, ¶¶ 14 and 61. The first random number is decrypted with the first secret cryptographic key. *See, e.g.*, Specification, Figs. 9A, 9B, 10, and ¶ 59. The second random number is encrypted with the first secret cryptographic key. *See, e.g.*, Specification, Figs. 9A, 9B, 10, and ¶ 61. A second challenge is then transmitted to the computing device, where the second challenge comprises the encrypted second random number. *See, e.g.*, Specification, Figs. 9A, 9B, 10, and ¶ 61.

B. SUMMARY OF DEPENDENT CLAIM 2

Claim 2, which depends from claim 1, is directed to the the “unique identifier.” Specifically, claim 2 recites that the unique identifier is a serial number of a physical token installed at the computing device. For support, *see, e.g.*, Specification, Fig. 3 and ¶ 39.

C. SUMMARY OF INDEPENDENT CLAIM 13

Independent claim 13 is directed to a communications system including a number of computing devices. *See, e.g.*, Specification, Figs. 2, 3 and ¶ 37. The system includes at least one authentication device. *Id.* Each authentication device includes a removable unique tamper-resistant physical token. *See, e.g.*, Specification, Figs. 2, 3 and ¶¶ 37-39. The token includes a random number generator configured to generate at least one random number different from a received random number. *See, e.g.*, Specification, Figs. 2, 3, ¶¶ 14, 37-39 and 61. The token

also includes a unique secret cryptographic key. *See, e.g.*, Specification, Figs. 2, 3, ¶¶ 14, 37-39. The token also includes a unique serial number. *Id.*

D. SUMMARY OF INDEPENDENT CLAIM 19

Claim 19 is directed to a cryptographic protocol for authenticating computing devices. For support, *see, e.g.*, Fig. 11 and ¶¶ 64-67. A first challenge is received from the computing device to be authenticated, where the first challenge includes a first random number and a unique identifier associated with that computing device. *See, e.g.*, Specification, Fig. 11 and ¶ 64. A first secret cryptographic key associated with the unique identifier is obtained. *See, e.g.*, Specification, Fig. 11 and ¶ 65. A second random number is generated, where the second random number is different from the first random number. *See, e.g.*, Specification, Fig. 11, ¶¶ 14 and 65. The first random number is encrypted with the first secret cryptographic key. *See, e.g.*, Specification, Fig. 11 and ¶ 65. A second challenge is transmitted to the computing device, where the second challenge includes the encrypted first random number and the second random number. *Id.*

E. SUMMARY OF DEPENDENT CLAIM 25

Claim 25, which depends from claim 19 by way of claims 20 and 21, further refines the cryptographic protocol by reciting additional exchanged and compared parameters. In particular, claim 25 recites receiving a third challenge from the computing device, where the third challenge includes the second random number encrypted with a second secret cryptographic key. *See, e.g.*, Specification, Fig. 11 and ¶ 67. The encrypted second random number is decrypted with the first secret cryptographic key. *Id.* The decrypted second random number is compared to the second random number to determine if a match exists. *Id.*

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues before the Board are:

- Whether claims 1, 2, 19 and 25 are unpatentable under 35 U.S.C. § 103(a) as allegedly being obvious over U.S. Patent No. 6,397,328 to Pitchenik *et al.* (“Pitchenik”) in view of U.S. Patent No. 5,473,689 to Eberhard (“Eberhard”); and
- Whether claim 13 is unpatentable under 35 U.S.C. § 103(a) as allegedly being obvious over Pitchenik in view of Eberhard and further in view of U.S. Published application No. 2004/0203590 to Shteyn (“Shteyn”).

Appellants note here that although the Office Action purports to reject claim 13 under 35 U.S.C. § 103(a) over Pitchenik in view of Eberhard (see Office Action, page 2), the Office Action only presents arguments and analysis of claim 13 as allegedly being obvious over Pitchenik in view of Eberhard and further in view of Shteyn (see Office Action, page 8). Appellants therefore consider claim 13 to be rejected only over the latter grounds.

VII. ARGUMENTS

A. THE OFFICE ACTION APPEARS TO IMPERMISSIBLY COMBINE MULTIPLE EMBODIMENTS OF PITCHENIK

Although far from clear, the Office appears to be combining different portions of multiple embodiments in presenting its rejections. In particular, the Office Action repeatedly cites portions of Pitchenik that disclose multiple embodiments. Regarding claim 1, for example, the Office Action cites Pitchenik, col. 2, l. 40 - col. 3, l. 28 and col. 4, ll. 32-67. *See* Office Action, pages 2-3. These passages refer to no fewer than seven (7) different embodiments:

The present invention provides a method for verifying that a host system is the expected host system once the PSD has been verified as the expected PSD. ... The present invention further provides alternate embodiments secure and reliable methods for verifying in the host system that the expected PSD is coupled to the

host system. In one embodiment, a message, such as a random number, is generated in the Host system and sent to the PSD. In one embodiment, the PSD encrypts the number and transmits it to the Host system. ... In an alternate embodiment, the random number is signed in the PSD. ...

In yet another embodiment, the PSD has a private key which is associated with a specific public key that is stored in the host PC. ...

In another embodiment, a random number is generated in the host system and encrypted with a PSD state identification number. ...

Pitchenik, col. 2, l. 40 - col. 3, l. 28 (emphasis added). The rejections of the remaining independent claims, 13 and 19, contain similar citations. *See* Office Action, pages 3-4 and 8-9.

Appellants have twice explicitly requested that the Office specify exactly which single embodiment is relied upon in forming the rejections. *See* Response to Office Action filed March 23, 2005, page 5, (III); and Response to Office Action filed August 23, 2005, page 8. The Office has not responded to these requests.

The Office's refusal to specify which embodiment it relies upon in rejecting the claims provides at least the appearance that the Office is improperly combining disparate embodiments in rejecting the present claims. However, multiple embodiments may not be combined in forming a rejection unless the requirements for generating such a combination under §103 are satisfied. In particular, combining different embodiments in the same reference requires at least a motivation for such combination. The Office has not provided any motivation for combining the disparate Pitchenik embodiments.

Appellants have been forced to respond to an unclear rejection by guessing at which embodiment is cited as prior art. Nevertheless, as discussed in detail below, no single Pitchenik embodiment, either alone or in combination with Eberhard and Shteyn, includes every limitation of the pending claims.

**B. CLAIMS 1, 2, 19 AND 25 ARE PATENTABLE OVER PITCHENIK
IN VIEW OF EBERHARD UNDER 35 U.S.C. § 103**

As discussed above in section VII(A), the Office Action cites no less than seven (7) different Pitchenik embodiments. For convenience of the Board, Appellants will refer to the Pitchenik embodiments cited in the Office Action using the following conventions:

- Embodiment 1: column 2, lines 40-56;
- Embodiment 2: column 2, lines 57-65;
- Embodiment 3: column 2, line 65 - column 3, line 3;
- Embodiment 4: column 3, lines 4-16;
- Embodiment 5: column 3, lines 17-28;
- Embodiment 6: column 4, lines 32 - 67.

Note that Embodiment 6 includes two suggestions for alternate embodiments (column 4, lines 44-46 and 55-56). However, these additional embodiments do not affect the analysis.

**1. Claim 1 Is Patentable Over Pitchenik In View Of Eberhard Under 35
U.S.C. § 103**

Appellants preface this section by noting that the Office Action's position is that Pitchenik discloses every limitation of independent claim 1 except those related to generating a random number that is *different* from a first random number. *See* Office Action, pages 2-3. For convenience of the Board, Appellants present independent claim 1 below, underlining those limitations that the Office admits are absent in Pitchenik:

1. A method of authenticating computing devices on a communications network comprising the steps of:
 - receiving a first challenge from a computing device, wherein said first challenge comprises an encrypted first random number and a unique identifier associated with said computing device;
 - obtaining a first secret cryptographic key associated with said unique identifier;
 - generating a second random number, wherein the second random number is different from the first random number;
 - decrypting said first random number with said first secret cryptographic key;

encrypting said second random number with said first secret cryptographic key; and
transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted said second random number.

See Office Action, pages 2-3 (“Pitchenik discloses ... generating a second random number...”). Because above presentation is meant to assist the Board only, nothing in Appellant’s characterization should be taken as an admission that any of the cited art actually does disclose any limitation in the present claims.

Thus, the Office’s position is that every protocol step recited in independent claim 1 is present in Pitchenik, except for that noted above. In particular, the Office maintains that Pitchenik discloses “generating a second random number,” but not a second random number different from a first random number. *See* Office Action, page 2.

Because the Office’s position is that every limitation of claim 1, except as noted above, is present in Pitchenik, the appeal of claim 1 may be disposed of by simply comparing the remaining limitations of claim 1 with the disclosure of Pitchenik. As will become apparent, none of the multiple embodiments of Pitchenik disclose the protocol steps *arranged as recited in claim 1*.

i. Pitchenik Fails To Disclose The Protocol Steps Of Claim 1

Embodiment 1 fails to disclose “generating” a second random number. Indeed Embodiment 1 fails to disclose *any random number whatsoever*. In Embodiment 1, Pitchenik discloses encrypting a message, sending it, decrypting it, and encrypting a second message, which is derived from the first message. Even if the first message comprises a first random number (and Appellants do not so concede), the fact that the second message is *derived* from the first message prevents the second message from containing a *random* number. The Office’s position is that decrypting a random number meets the limitation of generating such a random number.

See the Office Action mailed May 26, 2005, page 10. This is not a reasonable interpretation. Encrypting a message may be thought of as placing the message in a safe. Clearly, opening such a safe does not constitute “generating” the message continued therein.

Embodiments 2 and 3 fail to disclose a “second random number.” There is absolutely no hint of generating a second random number, let alone “transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted said second random number” as claimed.

Embodiment 4 is entirely irrelevant to claim 1 because it fails to disclose (1) any random number, or (2) sending anything that is encrypted. Thus, Embodiment 4 fails to disclose, *e.g.*, “receiving a first challenge from a computing device, wherein said first challenge comprises an encrypted first random number” or “transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted said second random number.”

Embodiment 5 fails to disclose at least two limitations of claim 1. First, Embodiment 5 fails to disclose “receiving a first challenge from a computing device, wherein said first challenge comprises ... a unique identifier associated with said computing device.” There is absolutely no hint or suggestion of transmitting a unique identifier. Second, Embodiment 5 fails to disclose any second random number, let alone “transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted said second random number,” as claimed.

Embodiment 6 fails to disclose “generating” a second random number. In Embodiment 6, Pitchenik discloses encrypting a random number, sending it, decrypting it, and then re-encrypting the *same random number*. The Office’s position is that decrypting a random number

meets the limitation of generating such a random number. *See* the Office Action mailed May 26, 2005, page 10. This is not a reasonable interpretation. As discussed above, encrypting a message may be thought of as placing the message in a safe. Clearly, opening such a safe does not constitute “generating” the message continued therein.

Further, Embodiment 6 fails to disclose “receiving a first challenge from a computing device, wherein said first challenge comprises ... a unique identifier associated with said computing device.” At most, Embodiment 6 discloses transmitting “data indicating status of the PSD based, for example a checksum of PSD transaction records stored as log files in Host PC 20” as an *alternative* to transmitting a random number. *See* Pitchenik, column 4, lines 36-40. Appellants maintain that “data indicating status of the PSD” does not meet the limitation of “a unique identifier associated with said computing device.” Moreover, there is absolutely no hint or suggestion of transmitting a challenge comprising *both* an encrypted random number and a unique identifier.

ii. **Eberhard Fails To Disclose Generating A Second Random Number Different From A First Random Number**

The Office relies on Eberhard for meeting the limitation of “generating a second random number, *wherein the second random number is different from the first random number.*” Eberhard fails to disclose this limitation.

Nowhere does Eberhard disclose, discuss, teach or suggest generating different random numbers. At most, Eberhard disclose generating two random numbers. Eberhard is absolutely silent regarding whether such random numbers are different. As such, it is entirely inappropriate to rely on Eberhard for this very feature.

iii. The Office's Motivation To Combine Is Flawed

The Office Action offers nothing but conclusory, unsupported statements as its alleged motivation to combine references in its rejection of claim 1. The Office concedes that Pitchenik does not disclose “generating a second random number, wherein the second random number is different from the first random number.” Office Action, page 3. The Office turns to Eberhard as allegedly filling the gap. In particular, the Office Action presents the following alleged motivation to combine Eberhard with Pitchenik:

- [1] It would have been obvious to one having ordinary skill in the art to generate different random numbers when two devices try to authenticate each other.
- [2] Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Eberhard within the system of Pitchenik because using two random numbers allows both devices to exclusively authenticate each other.

Office Action, page 3. These assertions are not motivations for combination. Instead, they are conclusions. Stating that “it would have been obvious” does not make it so. Indeed, the Office Action contains no actual motivation for combining Pitchenik with Eberhard. The statement [1] is, at best, a conclusory statement that assumes what it purports to prove. There is no answer to the crucial question: *Why* would someone want to generate *different* random numbers? Further, [2], in a conclusory manner, states that a combination of Pitchenik with Eberhard would have been obvious by relying on essentially a re-statement of [1]. That is, [2] is a conclusory statement that uses the conclusory statement [1] as its justification. This alleged motivation to combine cannot stand. The U.S. Patent Office cannot simply restate a claim limitation as grounds for combining references used to reject the claim at issue.

Furthermore, there is no expectation of success in combining Eberhard with Pitchenik. The design of cryptographic protocols is *not* a predictable art. Much care, experimentation and

testing is required to discover a cryptographic protocol that serves its intended purpose, which in this case is authentication. *See* Section V above. Arbitrarily swapping out parameters in a protocol will almost assuredly lead to an insecure protocol, *i.e.*, a protocol that does not perform its intended purpose. *See Id.* Accordingly, there is no expectation of success in importing features of Eberhard's protocol into that of Pitchenik.

2. Claim 2 Is Patentable Over Pitchenik In View Of Eberhard Under 35 U.S.C. § 103

Claim 2 recites that the “unique identifier [of claim 1] is a serial number of a physical token installed at said computing device.” Neither Pitchenik nor Eberhard disclose any type of physical token.

The present specification discusses the qualities of a physical token: “[t]he present invention [uses] ... physical keys in the form of easy-to-use adapters that attach to existing computing devices and wireless access points... These physical keys are secure, tamper-resistant physical tokens.” Specification, ¶ 36. Pitchenik lacks any discussion of such physical tokens.

As best understood by Appellants, the Office's position appears to be that a physical token is included somewhere in Pitchenik's Postage Security Device (“PSD”). The Office stakes out this position as follows:

[A]pplicant argues that Pitchenik reference does not disclose a tamper resistant physical token. However, Pitchenik discloses that the cryptographic key and unique ID are stored within the postage security device, which is a tamper resistant device. Therefore, the tamper-resistant physical token is included in the postage security device ready for authentication.

Office Action mailed May 26, 2005, page 10. This position is untenable. Standing alone, a key together with an ID do not constitute a “physical token.” The mere fact that Pitchenik stores a key and an ID somewhere in a PSD does not mean that that the storage location is a “physical

token.” Pitchenik could, for example, store a key and an ID on a permanent hard drive inside the PSD. Such a permanent hard drive is *not* a “physical token” as claimed. In short, the mere fact that Pitchenik discloses that a key and ID are located somewhere inside a PSD box does not address the limitation of “a physical token installed at said computing device.”

3. **Claim 19 Is Patentable Over Pitchenik In View Of Eberhard Under 35 U.S.C. § 103**

Appellants preface this section by noting the Office’s position that Pitchenik discloses every limitation of independent claim 19 except those related to generating a random number that is *different* from a first random number. *See* Office Action, page 3-4. For convenience of the Board, Appellants present independent claim below, underlining those limitations that the Office admits are absent in Pitchenik:

19. A method of authenticating computing devices on a communications network comprising the steps of:
- receiving a first challenge from a computing device, wherein said first challenge comprises a first random number and a unique identifier associated with said computing device;
 - obtaining a first secret cryptographic key associated with said unique identifier;
 - generating a second random number, wherein the second random number is different from the first random number;
 - encrypting said first random number with said first secret cryptographic key; and
 - transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted first random number and said second random number.

See Office Action, pages 3-4 (“Pitchenik discloses ... transmitting a second challenge to said computing device, wherein said second challenge comprises ... said second random number...”). Because the presentations are meant to assist the Board only, nothing in Appellant’s characterizations should be taken as an admission that any of the cited art actually does disclose any limitation in the present claims.

Because the Office's position is that every limitation of claim 19, except as noted above, is present in Pitchenik, the appeal of claim 19 may be disposed of by simply comparing the remaining limitations of the independent claims with the disclosure of Pitchenik. As will become apparent, none of the multiple embodiments of Pitchenik disclose the protocol steps *arranged as recited in claim 19*.

i. Pitchenik Fails To Disclose The Protocol Steps Of Claim 19

Embodiment 1 fails to disclose "generating" a second random number. Indeed Embodiment 1 fails to disclose *any random number whatsoever*. In Embodiment 1, Pitchenik discloses encrypting a message, sending it, decrypting it, and encrypting a second message, which is derived from the first message. Even if the first message comprises a first random number (and Appellants do not so concede), the fact that the second message is *derived* from the first message prevents the second message from containing a *random* number. The Office's position is that decrypting a random number meets the limitation of generating such a random number. *See* the Office Action mailed May 26, 2005, page 10. This is not a reasonable interpretation. As discussed above, encrypting a message may be thought of as placing the message in a safe. Clearly, opening such a safe does not constitute "generating" the message continued therein.

Embodiment 1 also fails to disclose transmitting an encrypted random number together with a random number in the clear. That is, Embodiment 1 fails to disclose "transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted first random number and said second random number." At most, Embodiment 1 discloses transmitting a single piece of information.

Embodiments 2 and 3 fail to disclose multiple random numbers. There is no hint of a second random number, let alone “a second challenge to said computing device, wherein said second challenge comprises said encrypted first random number and said second random number,” as claimed. Note that Embodiments 2 and 3 also fail to disclose any challenge containing two random numbers where one is encrypted and the other is not.

Embodiment 4 is entirely irrelevant to claim 1 because it fails to disclose (1) any random number, or (2) sending anything that is encrypted. Thus, Embodiment 4 fails to disclose, *e.g.*, “said first challenge comprises a first random number and a unique identifier associated with said computing device” or “transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted first random number and said second random number.”

Embodiment 5 fails to disclose at least two limitations of claim 19. First, Embodiment 5 fails to disclose “receiving a first challenge from a computing device, wherein said first challenge comprises ... a unique identifier associated with said computing device.” There is absolutely no hint or suggestion of transmitting a unique identifier. Second, Embodiment 5 fails to disclose any second random number, let alone “transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted said first random number and said second random number,” as claimed.

Embodiment 6 fails to disclose “generating” a second random number. In Embodiment 6, Pitchenik discloses encrypting a random number, sending it, decrypting it, and then re-encrypting the *same random number*. The Office’s position is that decrypting a random number meets the limitation of generating such a random number. *See* the Office Action mailed May 26,

2005, page 10. This is not a reasonable interpretation. As discussed above, encrypting a message may be thought of as placing the message in a safe. Clearly, opening such a safe does not constitute “generating” the message continued therein.

Further, Embodiment 6 fails to disclose “receiving a first challenge from a computing device, wherein said first challenge comprises ... a unique identifier associated with said computing device.” At most, Embodiment 6 discloses transmitting “data indicating status of the PSD based, for example a checksum of PSD transaction records stored as log files in Host PC 20” as an *alternative* to transmitting a random number. *See* Pitchenik, column 4, lines 36-40. Appellants maintain that “data indicating status of the PSD” does not meet the limitation of “a unique identifier associated with said computing device.” Moreover, there is absolutely no hint or suggestion of transmitting a challenge comprising *both* an encrypted random number and a unique identifier.

ii. **Eberhard Fails To Disclose Generating A Second Random Number Different From A First Random Number**

The Office relies on Eberhard for meeting the limitation of “generating a second random number, wherein the second random number is different from the first random number.” Eberhard fails to disclose this limitation.

Nowhere does Eberhard disclose, discuss, teach or suggest generating different random numbers. At most, Eberhard disclose generating two random numbers. Eberhard is absolutely silent regarding whether such random numbers are different. As such, it is entirely inappropriate to rely on Eberhard for this very feature.

iii. The Office's Motivation To Combine Is Flawed

The Office Action offers nothing but conclusory, unsupported statements as its alleged motivation to combine references in its rejection of claim 19. The Office concedes that Pitchenik does not disclose “generating a second random number, wherein the second random number is different from the first random number.” Office Action, page 3. The Office turns to Eberhard as allegedly filling the gap. In particular, the Office Action presents the following alleged motivation to combine Eberhard with Pitchenik:

- [1] It would have been obvious to one having ordinary skill in the art to generate different random numbers when two devices try to authenticate each other.
- [2] Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Eberhard within the system of Pitchenik because using two random numbers allows both devices to exclusively authenticate each other.

Office Action, page 4. These assertions are not motivations for combination. Instead, they are conclusions. Stating that “it would have been obvious” does not make it so. Indeed, the Office Action contains no actual motivation for combining Pitchenik with Eberhard. The statement [1] is, at best, a conclusory statement that assumes what it purports to prove. There is no answer to the crucial question: *Why* would someone want to generate *different* random numbers? Further, [2], in a conclusory manner, states that a combination of Pitchenik with Eberhard would have been obvious by relying on essentially a re-statement of [1]. That is, [2] is a conclusory statement that is uses the conclusory statement [1] as its justification. This alleged motivation to combine cannot stand. The U.S. Patent Office cannot simply restate a claim limitation as grounds for combining references used to reject the claim at issue.

Furthermore, there is no expectation of success in combining Eberhard with Pitchenik. The design of cryptographic protocols is *not* a predictable art. Much care, experimentation and

testing is required to discover a cryptographic protocol that serves its intended purpose, which in this case is authentication. *See* Section V above. Arbitrarily swapping out parameters in a protocol will almost assuredly lead to an insecure protocol, *i.e.*, a protocol that does not perform its intended purpose. *See Id.* Accordingly, there is no expectation of success in importing features of Eberhard's protocol into that of Pitchenik.

4. Claim 25 Is Patentable Over Pitchenik In View Of Eberhard Under 35 U.S.C. § 103

None of Embodiments 1-6 disclose a third challenge as recited in claim 25. Further, the Office does not rely on Eberhard as filling the gap. As such, the rejection of claim 25 is fatally flawed and must be reversed.

C. CLAIM 13 IS PATENTABLE OVER PITCHENIK IN VIEW OF EBERHARD AND FURTHER IN VIEW OF SHTEYN UNDER 35 U.S.C. § 103

Appellants preface this section by noting that the Office Action's position is that Pitchenik discloses every limitation of claim 13 except:

- generating a random number that is *different* from a first random number; and
- a physical token being *removable*.

See Office Action, page 8. For convenience of the Board, Appellants present claim 13 below, underlining those limitations that the Office admits are absent in Pitchenik.

13. A communications system comprising:
a number of computing devices, and
at least one authentication device,
wherein each authentication device includes a removable unique tamper-resistant physical token comprising
a random number generator configured to generate at least one random number different from a received random number,
a unique secret cryptographic key, and
and a unique serial number.

See Office Action, pages 8-9. Note that the Office insists that Pitchenik discloses a “removable unique tamper-resistant physical token,” but later admits that Pitchenik’s alleged physical token is not removable and instead relies on Eberhard for the removability feature. *See* Office Action, page 8. Because this presentation is meant to assist the Board only, nothing in Appellant’s characterizations should be taken as an admission that any of the cited art actually does disclose any limitation in the present claims.

Because the Office’s position is that every limitation of claim 13, except as noted above, is present in Pitchenik, the appeal of claim 13 may be disposed of by simply comparing the remaining limitations of claim 13 with the disclosure of Pitchenik.

As discussed above in section VII(A), the Office Action cites no less than seven (7) different Pitchenik embodiments. For convenience of the Board, Appellants will refer to the Pitchenik embodiments cited in the Office Action using the following conventions:

- Embodiment 1: column 2, lines 40-56;
- Embodiment 2: column 2, lines 57-65;
- Embodiment 3: column 2, line 65 - column 3, line 3;
- Embodiment 4: column 3, lines 4-16;
- Embodiment 5: column 3, lines 17-28;
- Embodiment 6: column 4, lines 32 - 67.

Note that Embodiment 6 includes two suggestions for alternate embodiments (column 4, lines 44-46 and 55-56). However, these additional embodiments do not affect the analysis.

1. Pitchenik Fails To Disclose A Physical Token

Pitchenik has absolutely no teaching, suggestion, consideration, discussion, or reference concerning a “physical token.” The present specification discusses the qualities of a physical token: “[t]he present invention [uses] ... physical keys in the form of easy-to-use adapters that attach to existing computing devices and wireless access points... These physical keys are

secure, tamper-resistant physical tokens.” Specification, ¶ 36. Pitchenik lacks any discussion of such physical tokens.

As best understood by Appellants, the Office’s position appears to be that a tamper-resistant “physical token comprising a random number generator, a unique secret cryptographic key, and a unique serial number” is included somewhere in Pitchenik’s postage security device (“PSD”).

The Examiner stakes out this position as follows:

[A]pplicant argues that Pitchenik reference does not disclose a tamper resistant physical token. However, Pitchenik discloses that the cryptographic key and unique ID are stored within the postage security device, which is a tamper resistant device. Therefore, the tamper-resistant physical token is included in the postage security device ready for authentication.

Office Action mailed May 26, 2005, page 10. This position is untenable. Standing alone, a key together with an ID do not constitute a “physical token.” The mere fact that Pitchenik stores a key and an ID somewhere in a PSD does not mean that that the storage location is a “physical token.” Pitchenik could, for example, store a key and an ID on a permanent hard drive inside the PSD. Such a permanent hard drive is *not* a “removable physical token.”

In short, the mere fact that Pitchenik discloses that a key and ID are located somewhere inside a PSD box does not meet the limitation of “at least one authentication device, wherein each authentication device includes a removable unique tamper-resistant physical token comprising a random number generator configured to generate at least one random number different from a received random number.”

2. Pitchenik Fails To Disclose Tamper-Resistance

Claim 13 recites “a removable unique tamper-resistant physical token.” Pitchenik has absolutely no teaching, suggestion, consideration, discussion, or reference concerning anything that is

“tamper-resistant.” At most, Pitchenik discloses in a completely generic manner that the entire system is “secure.” *See* Pitchenik, column 1, lines 51-53. Appellants strongly dispute that a generic disclosure of an entire system being “secure” amounts to a disclosure of a physical token being “tamper-resistant.” “Secure” does *not* imply “tamper-resistant.” For example, encrypted data stored on magnetic media might be considered “secure,” but are certainly *not* “tamper-resistant” because such data could easily be altered. In short, “secure” does *not* mean or imply “tamper-resistant.”

Furthermore, Pitchenik does not disclose that any removable physical token is tamper-resistant. Rather, the entire system of Pitchenik is referred to as being “secure,” although exactly how the system is “secure” is not specified. *See* Pitchenik, column 2, lines 34-39. The disclosure of Pitchenik cannot, therefore, be properly relied upon to reject claim 13, which specifies that the physical token is “tamper-resistant.” Because Pitchenik lacks any teaching regarding a “unique tamper-resistant physical token,” the rejection is improper and should be withdrawn.

3. Shteyn Fails To Disclose Tamper-Resistance

The Office relies on Shteyn as disclosing that “each tamper resistant token is removable.” *See* Office Action, pages 8-9. However, as discussed immediately above, Pitchenik completely fails to disclose any part of the limitation “a removable unique tamper-resistant physical token.” Thus, to properly fill the gap left by Pitchenik, Shteyn would have to disclose at least a tamper-resistant physical token.

Shteyn fails to disclose this limitation. The Office asserts that the Shteyn discloses “using a dongle installed via a USB to secure communications in a wireless network.” Office Action,

pages 9-10. However, Shteyn's dongle is *not* "tamper-resistant." *See* Shteyn, ¶ 27. A generic reference to "using a dongle ... to secure communication" does *not* amount to a teaching of a "removable unique tamper-resistant physical token." In the complete absence of such teaching, reliance on Shteyn is misplaced.

4. Shteyn Fails To Disclose A Physical Token Comprising A Random Number Generator

Shteyn's dongle does *not* contain a "random number generator." Nor has the Office provided any motivation for including a "random number generator" in a removable physical token. Accordingly, it is improper to rely on a combination of Pitchenik with Shteyn and Eberhard when none of these references disclose a random number generator included in a physical token and the Office fails to supply any motivation for doing so.

5. Eberhard Fails To Disclose Generating A Second Random Number Different From A First Random Number

Claim 13 recites "a random number generator configured to generate at least one random number different from a received random number." The Office admits that Pitchenik fails to disclose this feature. *See* Office Action, page 8. Instead, the Office relies on Eberhard for meeting this limitation.

Nowhere does Eberhard disclose, discuss, teach or suggest generating different random numbers. At most, Eberhard disclose generating two random numbers. Eberhard is absolutely silent regarding whether such random numbers are different. As such, it is entirely inappropriate to rely on Eberhard for this very feature.

6. **The Office's Motivation To Combine Eberhard With Pitchenik Is Flawed**

The Office Action offers nothing but conclusory, unsupported statements as its alleged motivation to combine references in its rejection of independent claim 13. The Office concedes that Pitchenik does not disclose “generating a second random number, wherein the second random number is different from the first random number.” Office Action, page 8. The Office turns to Eberhard as allegedly filling the gap. In particular, the Office Action presents the following alleged motivation to combine Eberhard with Pitchenik:

- [1] It would have been obvious to one having ordinary skill in the art to generate different random numbers when two devices try to authenticate each other.
- [2] Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Eberhard within the system of Pitchenik because using two random numbers allows both devices to exclusively authenticate each other.

Office Action, page 8. These assertions are not motivations for combination. Instead, they are conclusions. Stating that “it would have been obvious” does not make it so. Indeed, the Office Action contains no actual motivation for combining Pitchenik with Eberhard. The statement [1] is, at best, a conclusory statement that assumes what it purports to prove. There is no answer to the crucial question: *Why* would someone want to generate *different* random numbers? Further, [2], in a conclusory manner, states that a combination of Pitchenik with Eberhard would have been obvious by relying on essentially a re-statement of [1]. That is, [2] is a conclusory statement that uses the conclusory statement [1] as its justification. This alleged motivation to combine cannot stand. The U.S. Patent Office cannot simply restate a claim limitation as grounds for combining references used to reject the claim at issue. The Office Action simply fails to provide proper motivation to combine Pitchenik with Eberhard.

Furthermore, there is no expectation of success in combining Eberhard with Pitchenik. The design of cryptographic protocols is *not* a predictable art. Much care, experimentation and testing is required to discover a cryptographic protocol that serves its intended purpose, which in this case is authentication. *See* Section V above. Arbitrarily swapping out parameters in a protocol will almost assuredly lead to an insecure protocol, *i.e.*, a protocol that does not perform its intended purpose. *See Id.* Accordingly, there is no expectation of success in importing features of Eberhard's protocol into that of Pitchenik.

7. The Office's Motivation To Combine Shteyn With Pitchenik And Eberhard Is Flawed

The Office Action concedes that Pitchenik fails to disclose that "each tamper-resistant physical token is removable." Office Action, page 8. Turning to Shteyn as allegedly filling the gap, the Office writes:

- [1] It would have been obvious to one having ordinary skill in the art to store identifications information and cryptographic key into the hardware key while authentication takes place between a mobile terminal and an access point.
- [2] Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shteyn within the combination of Pitchenik-Eberhard because dongle is well known in the art for providing security parameters within network.

Office Action, page 9. Here again, [1] is no more than a conclusory statement that assumes what it purports to prove. There is no reasoning as to why "it would have been obvious," only a bare statement that it would have been. There is no answer to the crucial question: *Why* would it be obvious to store a unique serial number and a unique secret cryptographic key in Shteyn's dongle? Moreover, neither the present claims nor the disclosure of Pitchenik are directed to a "mobile terminal and an access point." As such, it is improper to use the same as justification for any alleged obviousness. As to [2], this statement is at best a conclusory shotgun assertion that

is unsupported by any art of record. As such, neither [1] nor [2] are proper motivation for combining Pitchenik with Shteyn.

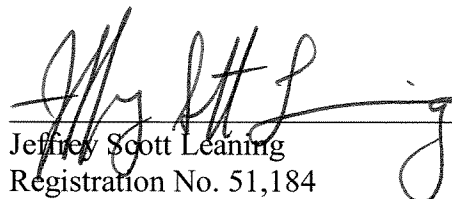
Moreover, the alleged motivation to combine Shteyn with Pitchenik and Eberhard fails to address the inclusion of a random number generator contained in a physical token. As discussed above, no single cited reference discloses a physical token comprising a random number generator. In the complete absence of any motivation for inserting a random number generator into a physical token, the rejection of a claim reciting a “tamper-resistant physical token comprising a random number generator” is entirely unsupported and must be reversed.

VIII. CONCLUSION

In view of the foregoing, Appellant respectfully requests that the Board of Patent Appeals and Interferences reverse the prior art rejections set forth in the Office Action, and allow all of the pending claims.

Respectfully submitted,

Date: July 31, 2006



Jeffrey Scott Leaning
Registration No. 51,184

Hunton & Williams LLP
1900 K. St., NW, Suite 1200
Washington, D.C. 20006-1109
Tel: (202) 955-1500
Fax: (202) 778-2201

APPENDIX - Pending Claims

Claims 1-11 and 13-28 are currently pending and subject to this appeal.

1. A method of authenticating computing devices on a communications network comprising the steps of:
 - receiving a first challenge from a computing device, wherein said first challenge comprises an encrypted first random number and a unique identifier associated with said computing device;
 - obtaining a first secret cryptographic key associated with said unique identifier;
 - generating a second random number, wherein the second random number is different from the first random number;
 - decrypting said first random number with said first secret cryptographic key;
 - encrypting said second random number with said first secret cryptographic key; and
 - transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted said second random number.
2. The method of claim 1, wherein said unique identifier is a serial number of a physical token installed at said computing device.
3. The method of claim 2, wherein said step of obtaining a first secret cryptographic key comprises the step of
 - retrieving a pre-stored record associated with said serial number, wherein said record comprises said first secret cryptographic key.
4. The method of claim 3, wherein said step of obtaining a first secret cryptographic key comprises the step of

receiving a key database file comprising a number of records, wherein each record is associated with a unique physical token and comprises a unique secret cryptographic key and a unique serial number.

5. The method of claim 4, wherein said unique secret cryptographic key is created from a random number generated at initialization of said token.
6. The method of claim 1, further comprising the steps of:
 - decrypting said first challenge with a network receive cryptographic key; and
 - encrypting said second challenge with a network send cryptographic key.
7. The method of claim 3, wherein said step of decrypting said encrypted first random number results in a first value, and further comprising the step of
 - disallowing said computing device to communicate with other computing devices on said network if said first value is a null value.
8. The method of claim 7, wherein
 - allowing said computing device to communicate with other computing devices on said network if said first value is not a null value.
9. The method of claim 7, further comprising the step of
 - decrypting said second challenge with a network receive cryptographic key.
10. The method of claim 8, further comprising the step of
 - decrypting said encrypted second random number with a second secret cryptographic key.

11. The method of claim 10, wherein said second secret cryptographic key is stored within said physical token.
12. (Cancelled)
13. A communications system comprising:
 - a number of computing devices, and
 - at least one authentication device,
 - wherein each authentication device includes a removable unique tamper-resistant physical token comprising
 - a random number generator configured to generate at least one random number different from a received random number,
 - a unique secret cryptographic key, and
 - and a unique serial number.
14. The system of claim 13, wherein each client device or authentication device further includes a wireless communications transceiver to communicate on a wireless network.
15. The system of claim 14, wherein said wireless network is Wi-Fi network.
16. The system of claim 15, wherein said authentication device is an access point.
17. The system of claim 13, wherein each tamper-resistant physical token is installed via a USB interface.
18. The system of claim 16, wherein said access point includes a database file comprising said serial numbers and secret cryptographic keys associated with said tokens.

19. A method of authenticating computing devices on a communications network comprising the steps of:

receiving a first challenge from a computing device, wherein said first challenge comprises a first random number and a unique identifier associated with said computing device;

obtaining a first secret cryptographic key associated with said unique identifier;

generating a second random number, wherein the second random number is different from the first random number;

encrypting said first random number with said first secret cryptographic key; and

transmitting a second challenge to said computing device, wherein said second challenge comprises said encrypted first random number and said second random number.

20. The method of claim 19, wherein said unique identifier is a serial number of a physical token installed at said computing device.

21. The method of claim 20, wherein said step of obtaining a first secret cryptographic key comprises the step of

retrieving a pre-stored record associated with said serial number, wherein said record comprises said first secret cryptographic key.

22. The method of claim 21, wherein said step of obtaining a first secret cryptographic key comprises the step of

receiving a key database file comprising a number of records, wherein each record is associated with a unique physical token and comprises a unique secret cryptographic key and a unique serial number.

23. The method of claim 22, wherein said unique secret cryptographic key is created from a random number generated at initialization of said token.
24. The method of claim 19, further comprising the steps of:
- decrypting said first challenge with a network receive cryptographic key; and
 - encrypting said second challenge with a network send cryptographic key.
25. The method of claim 21, further comprising the steps of:
- receiving a third challenge from said computing device, wherein said third challenge comprises said second random number encrypted with a second secret cryptographic key;
 - decrypting said encrypted second random number with said first secret cryptographic key; and
 - comparing said decrypted second random number to said second random number to determine if a match exists.
26. The method of claim 25, wherein
- if a match exists between said decrypted second random number and said second random number,
 - allowing said computing device to communicate with other computing devices on said network,
 - otherwise if a match does not exist,
 - disallowing said computing device to communicate with other computing devices on said network.
27. The method of claim 25, further comprising the step of
- decrypting said third challenge with a network receive cryptographic key.

28. The method of claim 25, wherein said second secret cryptographic key is stored within said physical token.

APPENDIX - Evidence

None.

APPENDIX - Related Proceedings

None.